REMARKS

Claims 1-39 are pending in the present application. Claims 4, 14-27, and 30 are amended. Reconsideration of the claims is respectfully requested.

I. Examiner Interview

Applicant thanks Examiner Shubert for the courtesies extended to Applicant's representative during the July 8, 2005 telephone interview. During the interview, the Examiner discussed the rejection of claims 1, 14 and 27 under 35 U.S.C. 102(e) with Applicant's representative.

II. 35 U.S.C. § 112, Second Paragraph

The examiner has rejected claims 4, 17 and 30 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter, which applicants regard as the invention. The Office Action states that the claims disclose "said DTD file" and "said plurality of tags" where neither a "DTD file" nor a "plurality of tags" is disclosed in claims 1, 14, and 27 on which claims 4, 17 and 30 depend. Claims 4, 17 and 30 have been amended to claim "said plurality of different elements" and to depend from claims 3, 16 and 29, which recite "a plurality of different elements in said DTD file." Claims 3, 16 and 29 depend from claims 2, 15 and 28, which recite "a DTD file."

The Examiner has also rejected claim 27 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention because a "system for automatically configuring an IP security tunnel" was not disclosed in the claim. Claim 27 has been amended to recite as follows:

> 27. A data processing system for automatically configuring IP security tunnels, comprising:
> a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types; and
> said system for automatically configuring an IP security tunnel utilizing said security policy specification format.

Therefore the rejection of claims 4, 17, 27 and 30 under 35 U.S.C. § 112, second paragraph has been overcome.

III. 35 U.S.C. § 102, Anticipation, Claims 1, 5-14, 18-27 and 31-39

The examiner has rejected claims 1, 5-14, 18-27 and 31-39 under 35 U.S.C. § 102(e) as being anticipated by D'Sa (U.S. Patent Publication No. 2002/0178355) (hereinafter "*D'Sa*"). This rejection is respectfully traversed.

> As to claims 1, 14 and 27, the Office Action states:
>
> As per claims 1, 14, and 27, the applicant described a data processing system for defining a configuration of IP security tunnels comprising the following limitations which are met by D'Sa:
>
> a) a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machines ([0041], Fig.2);
>
> b) said system for automatically configuring an IP security tunnel utilizing said security policy specification format ([0042], Fig. 2);
>
> The applicant should note that the ideas of the instant invention have already been expressed in D'Sa. Though D'Sa maintains some of the same inventors as the instant invention, the inventive entity is different.

Office Action dated April 21, 2005, page 3.

Claim 1, which is representative of other rejected independent claims 18 and 31, with respect to similarly recited subject matter, states as follows:

> 1. A method in a data processing system for automatically configuring IP security tunnels, said method comprising the steps of:
>
> establishing a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types; and
>
> defining a configuration of an IP security tunnel utilizing said security policy specification format.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 194). Anticipation focuses on whether a claim reads on the product or process

a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983).

D'Sa does not teach each and every feature of the claims arranged as they are in the claims. Specifically, *D'Sa* does not teach automatically configuring IP security tunnels by "establishing a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types; and defining a configuration of an IP security tunnel utilizing said security policy specification format," as is recited in claim 1.

D'Sa does not teach or disclose "establishing a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types," as is recited in claim 1. The Examiner alleges this feature is taught by *D'Sa* at [0041] and Figure 2.

Figure 2 in *D'Sa* is shown as follows:

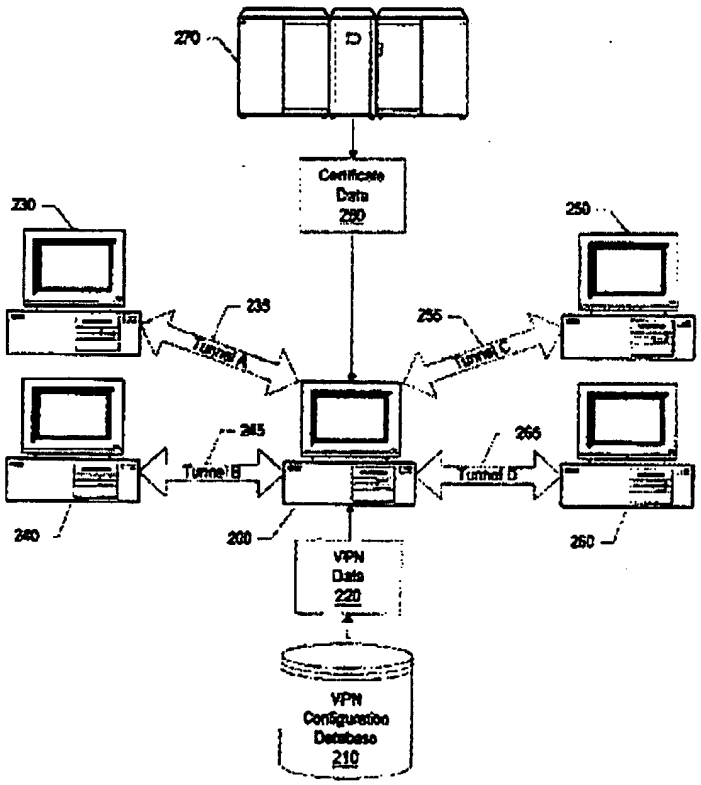


Figure 2

As can be seen **Figure 2** does not show the establishing step of claim 1 much less a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types. This figure shows computers, and tunnels used to transfer data. The figure also shows certificate data, VPN data, and a VPN database. Nowhere is a security policy specification format shown, much less one that is capable of being utilized by a plurality of different operating systems and a plurality of different machine types. Further, nothing is present in Figure 2 to teach or disclose the establishing step using this security policy specification format.

Next, *D'Sa* teaches as follows:

> FIG. 2 shows a diagram of tunnels being created between a computer and other computers using VPN configuration data and certificate data. Computer system 200 establishes various tunnels used to securely transmit data to and from other computer systems. Computer systems that computer system 200 wishes to securely communicate with over a VPN are identified in VPN configuration database 210. VPN data 220 contains information for connecting with a particular computer system. Using VPN configuration database 210, any number of VPNs can be established between computer system 200 and other computer systems. Some VPNs use certificate data 280 supplied by a trusted third party computer system 270. The use of a trusted third party aids in authenticating users and ensuring that an impostor does not take the place of another computer system.
>
> In the example shown, computer system 200 establishes tunnel A 235 securely connecting first computer system 230 with computer system 200. Likewise, tunnel B 245 securely connects second computer system 240 with computer system 200, tunnel C 255 securely connects third computer system 250 with computer system 200, and tunnel D 265 securely connects fourth computer system 260 with computer system 200. Each of these computer systems, 230, 240, 250, and 260, have identification information and authentication information stored in VPN configuration database 210.

D'Sa, [0040] and [0041].

Here, *D'Sa* teaches establishing tunnels between computer systems that are identified in a VPN configuration database containing information for connecting with the particular computer system. *D'Sa* discloses utilization of the information contained in the configuration database to establish VPNs for transmission of data between the computer systems identified in the database. However, *D'Sa* does not teach

"automatically configuring IP security tunnels" or "a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types," as is recited in claim 1. In fact, nothing is present in any section of *D'Sa* that teaches or discloses automatically configuring IP security tunnels or establishing a standard format for configuring IP security tunnels as recited in claim 1.

D'Sa does not teach or suggest "defining a configuration of an IP security tunnel utilizing said security policy specification format," as is recited in claim 1. The Examiner believes that this feature is taught in Figure 2. Figure 2 discloses that security tunnels are present between computers, but in no way provides any teaching or disclosure for defining a configuration of an IP security tunnel utilizing said security policy specification format.

The examiner believes that the defining step is taught in the following section of *D'Sa*:

> FIG. 3 shows a database diagram of tables used in configuring tunnels between the computer and other computer systems. VPN configuration database 300 is shown with four tables. Endpoints table 310 includes a list of configured tunnels between the computer system and other computer systems. One end of each endpoint identifies the computer system, while the other end of the endpoint identifies a remote computer. Each of the computers included in endpoints table 310 is identified with an identifier, such as an address. In addition, endpoints table 310 includes IP addresses for the remote computer systems. An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example 1.160.10.240 could be an IP address. Within an isolated network, IP addresses can be assigned at random so long as each one is unique. However, connecting a private network to the Internet requires using registered IP addresses (called Internet addresses) to avoid duplicates. The four numbers in an IP address are used in different ways to identify a particular network and a host on that network. Finally, endpoints table 310 includes a flag indicating whether a Certificate Revocation List (CRL) is used to check whether a given certificate has been revoked. Other valid ID types include FQDN, user@FQDN, distinguished names, and key IDs.

D'Sa, [0042].

As can be seen, this cited portion of *D'Sa* discloses a configuration database containing a list of configured tunnels between a computer system and a remote computer system to

determine a compatible authentication system. Although *D'Sa* appears to teach use of information in a configuration database for selecting an access method for computer systems requesting a VPN, *D'Sa* does not teach automatically configuring a security tunnel or utilizing a standardized security policy format capable of being used by a plurality of different operating systems as recited in claim 1.

D'Sa teaches:

> It has been discovered that a configuration tool can be provided to allow a computer system to be a member of multiple virtual private networks (VPSs). A database is included to store information about the various tunnels that can be used from the local computer system. An endpoints table includes a list of the configured tunnels. This list includes local-remote pair data with identifying information for each machine. A policy table is used to determine which access method(s) are used to connect the local computer system to the remote computer system. In addition, a preference order is provided in order to use multiple access methods in a preferred order. Two additional table include key information regarding the connection between the local and remote computer systems. A pre-shared keys table includes pre-shared key information, while a digital certificate table includes public key information and other digital certificate information.

D'Sa, [0021].

As shown above, *D'Sa* teaches selection of an access method by utilizing information in a configuration database regarding various tunnels that can be used by the computer systems requesting a VPN, including a list of already configured tunnels, a preference order for access methods where multiple access methods are available and connection information for the remote computer system. *D'Sa* does not teach or suggest a standardized format utilized in configuring IP security tunnels. Thus, *D'Sa* does not teach or disclose "defining a configuration of an IP security tunnel utilizing said security policy specification format," as in claim 1.

Therefore, *D'Sa* fails to teach each and every feature recited in claim 1. Other independent claims 14 and 27, which recite subject matter addressed above with regard to claim 1, are distinguishable over *D'Sa* based on the same rationale set forth above with regard to claim 1. In addition, independent claim 14 recites additional features not suggested by the reference. Amended claim 14 recites " a computer usable medium having computer usable program code for defining a configuration of IP security

tunnels." As discussed above, *D'Sa* merely teaches selection of an access method by utilizing information in a configuration database regarding various tunnels that can be used by a computer system requesting a VPN. There is nothing in any section of *D'Sa* that teaches or discloses "defining a configuration of IP security tunnels," as is claimed in independent claim 14. Therefore, *D'Sa* does not teach each and every feature of independent claim 14.

By virtue of their dependency on independent claims 1, 14, and 27, *D'Sa* does not teach each and every feature of dependent claims 5-13, 18-26, and 31 -39. Additionally, claims 5-3, 18-26, and 31-39 claim other additional combinations of features not suggested by the reference.

For example, with respect to claims 6, 11, 16, 24, 29, and 37, the Examiner alleges that *D'Sa* discloses a protection element at paragraph [0099], which states as follows:

> Depending on the authentication method used, key values are fetched from Public/Private Keys database 740 and Pre-Shared Keys database 745. For authentication methods that use public key encryption, Public/Private Keys database 740 is used. The Public/Private Keys database includes local private keys and corresponding digital certificates which contain the corresponding public key of the local ID and signing certificates including public keys corresponding to the signing certificates.

D'Sa, [0099].

In a VPN, computer systems can use pre-shared key encryption and a combination of private key, which is known only to the user's computer, and public key, which is given by the user's computer to any other computer that wants to communicate securely with it. *See D'Sa,* paragraph [0011]-[0012]. This section of *D'Sa* discloses fetching key values from a Public/Private Keys database and a Pre-Shared Keys database for authentication. However, there is nothing in this, or any other section of *D'Sa*, that teaches "a protection element in said security policy specification format, said protection element including a listing of IKE transforms," as is recited in claims 6, 11, 16, 24, 29, and 37.

As to claims 11, 24, and 37 the Examiner alleges that *D'Sa* teaches an IPsec proposal element, an IPsec authentication header element, and an IPsec protection element at paragraphs [0071], [0072], and [0146], which are as follows:

> Initiator Proposal List Index—an index to a initiator proposal list record (see Proposal List 725, below). If the Initiator Proposal List Index is null then initiation with the remote ID is not allowed (i.e., the system only acts as a responder to the remote ID).
>
> Responder Proposal List Index—an index to a responder proposal list record (see Proposal List 725, below). If this value is null, then response is not allowed (i.e., system only acts as an initiator when dealing with the remote ID). If both the Initiator Proposal List Index and the Responder Proposal List Index values are null, then no negotiation is allowed between the systems.

D'Sa, [0071]-[0072].

> The number authentication header (AH) Transforms, if this value is 0 then AH will not be proposed.

D'Sa, [0146].

Here, *D'Sa* discloses an Initiator Proposal List Index and a Responder Proposal List Index regarding the method of *D'Sa* by which an initiating computer proposes one or more authentication methods and a responder computer selects an authentication method from the initiator's proposal list. The above cited portions of *D'Sa* does not disclose any teachings regarding the Internet Protocol Security Protocol (IPsec) or "an IPsec proposal element, an IPsec ESP protocol element, an IPsec authentication header element, and an IPsec protection element" in a security policy specification format, as is claimed in claims 11, 24 and 37.

In regards to claims 12-13, 25-26, and 38-39, the Examiner states that *D'Sa* describes the step of automatically configuring an IP security tunnel utilizing the security policy specification format at *D'Sa*, paragraphs [0040] and [0041], which are set forth above. Here, *D'Sa* discloses establishing a VPN between a computer system and remote computer systems by using a configuration database containing identification data and authentication information for the computer system and the remote computer systems. However, *D'Sa* does not disclose a standardized format or "automatically configuring an IP security tunnel utilizing said security policy specification format," as is recited in claims 12, 15, and 38. Consequently, it is respectfully urged that the rejection of claims 1, 5-14, 18-27, and 31-39 have been overcome.

Therefore, the rejection of claims 1, 5-14, 18-27 and 31-39 under 35 U.S.C. § 102 has been overcome.

Furthermore, *D'Sa* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. *D'Sa* actually teaches away from the presently claimed invention because it teaches utilization of a list of already configured tunnels in the Endpoints table of the configuration database and preference data for use in determining a compatible access policy as opposed to automatically configuring an IP security tunnel by establishing a security policy specification format capable of being utilized by a plurality of different operating systems and defining a configuration of an IP security tunnel utilizing the security policy specification format, as in the presently claimed invention. Absent the examiner pointing out some teaching or incentive to implement *D'Sa* and automatically configuring IP security tunnels by establishing a security policy specification format for defining a configuration of an IP security tunnel, one of ordinary skill in the art would not be led to modify *D'Sa* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *D'Sa* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

IV. 35 U.S.C. § 102, Anticipation, Claims 1, 14 and 27

The examiner has rejected claims 1, 14 and 27 under 35 U.S.C. § 102(e) as being anticipated by Bendinelli (U.S. Patent No. 6,631,416) (hereinafter "*Bendinelli*"). This rejection is respectfully traversed.

> As to claims 1, 14 and 27, the Office Action states:
>
> As per claims 1, 14, and 27, the applicant describes a data processing system for defining a configuration of IP security tunnels with the following limitations which are met by Bendinelli:
>
> a) a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types (Col 17, lines 36-63);
>
> b) said system for automatically configuring an IP security tunnel (Col 17, lines 36-63);

Office Action dated April 21, 2005, page 4.

Bendinelli does not teach or disclose automatically configuring IP security tunnels by "establishing a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types; and defining a configuration of an IP security tunnel utilizing said security policy specification format," as is recited in claim 1. The Examiner alleges that this feature is taught by *Bendinelli* at column 17, lines 36-63, which is as follows:

> FIG. 3 shows an exemplary flowchart for initially registering one or more gateways with the control system 175. Referring to FIGS. 1 and 3, the user may register at least one of the gateways 150-153 with the control system 175 (step 310) and define a configuration for the registered gateways 150-153 (step 320). In one embodiment, the user may contact the control system 175 through the Internet using a web browser to specify a particular configuration for a gateway. This specified configuration information may include a name for the gateway and a name for the virtual private network. This name for the virtual private network will hereinafter be referred to as the virtual private network's domain name.
>
> The control system 175 may use the specified configuration to assemble code and information, such as program code and textual information (e.g., Extensible Markup Language also referred to as "XML"), in the form of a disk image (step 330). This disk image may include all the program code and information needed to configure gateways 150-153 for establishing one or more virtual private networks established over communication channel 120. The disk image may then be provided to the user and installed on a processor, such as a personal computer or a general-purpose computer (step 340). When the processor reboots, it uses the information provided in the disk image to configure itself as a gateway capable of establishing secure tunnels to the control system 175.

Bendinelli, column 17, lines 36-63.

Here, *Bendinelli* discloses the process whereby a user initially registers with a control system. According to *Bendinelli*, a user may contact a control system, such as a network operations center, to establish a VPN. The user provides configuration information to the control center, such as a name for the gateway and a name for the VPN, which is referred to by *Bendinelli* as a VPN domain name. The control system uses the configuration information to provide a program code to the user for installation on the user's computer. The program code, once installed, enables configuration of a gateway. *Bendinelli* teaches:

> [A] prospective user or customer may contact a mediation point or a control system, such as a network operations center via a base network, such as the Internet, and indicate a desire to establish one or more virtual private networks. After answering a series of questions posed by the network operations center, the user receives program code and information for loading onto one or more processors, such as personal computers. The program code and information may be in the form of a disk, such as an optical disk or floppy disk, downloaded over the Internet and onto a disk, or installed directly over the Internet on to a computer. The program code may be distributed to other computers at other desired sites user sites as well. Alternatively, the program code and information may be preinstalled on a computer and delivered to the user.
>
> The user then runs or boots a computer with the provided code and information. When the computer is booted, it thereafter communicates with the network operations center over the Internet to receive further information such that the computer is configured as a gateway or a computer capable of participating in one or more virtual private networks enabled by the network operations center over a base network, such as the Internet.

Bendinelli, column 10, line 61-column 12, line 16.

As is shown above, *Bendinelli* does not describe automatic configuration of a security tunnel utilizing a standardized format. According to the teachings of *Bendinelli*, a user registering with a control system requests establishment of a VPN. The control system requests configuration data from the user and provides a program code for installation on the user's computer to enable a VPN. In contradistinction, the presently claimed invention in claim 1 claims "a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types; and defining a configuration of an IP security tunnel utilizing said security policy specification format. Therefore, *Bendinelli* does not teach each and every feature of independent claim 1.

Independent claims 14 and 27 recite similar subject matter addressed above with respect to claim 1. Therefore claims 14 and 27 are distinguishable over *Bendinelli* under the same rationale as discussed above with regard to claim 1. Therefore, the rejection of claims 1, 14 and 27 under 35 U.S.C. § 102 has been overcome.

Furthermore, *Bendinelli* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. *Bendinelli* actually teaches

away from the presently claimed invention because it teaches a user registering with a control system as opposed to a standardized security policy specification format for configuring an IP security tunnel, as in the presently claimed invention. Absent the examiner pointing out some teaching or incentive to implement *Bendinelli* and automatically configuring an IP security tunnel utilizing a security policy specification format, one of ordinary skill in the art would not be led to modify *Bendinelli* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *Bendinelli* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

V. 35 U.S.C. § 103, Obviousness

The examiner has rejected claims 2-4, 15-17, and 28-30 under 35 U.S.C. § 103(a) as being unpatentable over *Bendinelli* in view of Pfeiffer (Pfeiffer, Ralph I. March 2, 1999. XML Tutorials for Programmers. retrieved from http://www.informatik.hu-berlin.de/~xing/Lib/RIP-writing.pfg) (hereinafter "*Pfeiffer*"). This rejection is respectfully traversed.

> As to claims 2-4, 15-17 and 28-30, the Office Action states:
>
> As per claims 2-4, 15-17, and 28-30, the applicant described the system of claims 1, 14, and 27, which are met by Bendinelli (see above), with the following limitation which is met by Bendinelli in view of Pfeiffer:
>
> Further comprising said security policy specification format being established as a DTD file (Bendinelli: Col 17, lines 36-63; Pfeiffer: pages 5-6);
>
> Bendinelli discloses all the limitations of independent claims 1, 14, and 27. However, Bendinelli does not disclose the use of a DTD file. Instead, Bendinelli discloses the use of an XML file for maintaining security policy specification. The applicant discloses the idea of using a DTD file which mutates into an XML file.
>
> Pfeiffer discloses that it is common in the art to maintain a DTD file with an XML document because a DTD file, through tags, provides grammar rules which increase organization and allow for validation of an XML document. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Pfeiffer with those of Bendinelli and add the use of DTD files with XML files because doing so increases organization and allows for validation of an XML file.

Office Action dated April 21, 2005, page 5.

In the above cited portion of the Office Action, the Examiner states that applicant discloses the idea of using a DTD file which mutates into an XML file. However, applicant does not claim a DTD file which mutates into an XML file in the presently claimed invention, as recited in claims 2-4, 15-17, and 28-30. For example, in claims 4, 17, and 30, which are the only claims that specifically claim an XML file, applicant claims as follows:

> 2. The method according to claim 3, further comprising the steps of:
> generating an XML file utilizing a plurality of said plurality of different elements included within said DTD file; and
> processing said XML file to automatically configure an IP security tunnel.

As is shown above, applicant claims "generating an XML file" using elements within a DTD file, rather than a DTD file mutating into an XML file, as suggested by Examiner.

Claims 2-4, 15-17, and 28-30 are dependent on independent claims 1, 14, and 27. As shown above, each and every feature of the independent claims are not show in Bendinelli. Also, for the same reasons stated above, this reference cannot be modified in the manner necessary to reach the presently claimed invention in the independent claims. Therefore, a combination of *Bendinelli* with *Pfeiffer* would not reach the presently claimed invention. Thus, these claims are patentable over *Bendinelli* and *Pfeiffer* for at least the reasons noted above with regards to claims 1, 14, and 27.

These claims also include additional feature that are patentable. Dependent claim 2, which is representative of other rejected dependent claims 3-4, 16-17, and 28-30, with respect to similarly recited subject matter, recites as follows:

> 2. The method according to claim 1, further comprising the step of establishing said security policy specification format as a DTD file.

The Examiner admits that *Bendinelli* does not disclose the use of a DTD file, but states that *Bendinelli* discloses the use of an XML file for maintaining security policy specification. As discussed above, *Bendinelli* merely teaches that a user may register with a control system, request establishment of a VPN, provide configuration information to the control system, and install program code provided by the control system on the user's computer to establish the VPN. *Bendinelli* teaches:

> [T]he user may contact the control system 175 through the Internet using a web browser to specify a particular configuration for a gateway. This specified configuration information may include a name for the gateway and a name for the virtual private network. This name for the virtual private network will hereinafter be referred to as the virtual private network's domain name.
>
> The control system 175 may use the specified configuration to assemble code and information, such as program code and textual information (e.g., Extensible Markup Language also referred to as "XML"), in the form of a disk image (step 330). This disk image may include all the program code and information needed to configure gateways 150-153 for establishing one or more virtual private networks established over communication channel 120. The disk image may then be provided to the user and installed on a processor, such as a personal computer or a general-purpose computer (step 340).

Bendinelli, column 17, lines 42-60.

Although *Bendinelli* teach that a program code may be an XML file, *Bendinelli* does not teach establishing a standard format capable of being used by any operating system and any machine type to automatically configure IP security tunnels, rather than manually configuring a tunnel by directly inputting the necessary parameters for the tunnel. There is nothing in any section of *Bendinelli* that teaches or suggests a standardized format for automatically configuring IP security tunnels, where the standardized format is a DTD file. Therefore, *Bendinelli* fails to teach or suggest "establishing said security policy specification format as a DTD file," as is recited in dependent claims 2, 15, and 28.

Applicant respectfully submits the references cannot be combined to produce the claimed invention. While *Pfieffer* may teach that it is common to maintain a DTD file with an XML document, *Pfieffer* does not teach or suggest establishing a security policy specification format as a DTD document. *Pfieffer* teaches:

> If you do create new tags, you must define, or constrain, them by writing grammar rules, which the tags must obey. Also called a **Document Type Declaration (DTD)**, these grammer rules are defined in the XML specification. They specifiy:
>
> - which tags are allowed within certain other tags
> - which tags and attributes are optional
>
> With regard to a DTD, an XML document can do any of the following:
>
> - Refer to a DTD, using a URI.
> - Include a DTD inline as part of the XML document.

- Omit a DTD altogether. Without a DTD, an XML document can be checked for well-formedness, but not for validity.

An XML document is **valid** if its contents conforms to the rules in its DTD. Validity allows an application to make sure the XML data is complete, is formatted properly, and has appropriate attribute values. It also allows an application to *construct* valid XML that conforms to that DTD, which is a very powerful feature.

Pfeiffer, page 6 of 14.

Pfeiffer merely discloses utilization of a DTD file with an XML document. Such teachings do not fairly teach or suggest a standardized format established as a DTD file for automatically configuring IP security tunnels, as in claim 2. Thus, although it may be common to maintain DTD files with XML files, it is not common to establish a security policy specification format as a DTD file. Nor does *Pfieffer* teach or suggest the establishing a security policy specification format as a DTD file, as in claim 2. Therefore, teachings of *Pfieffer* are insufficient to make up for the deficiencies of *Bendinelli*.

The proposed combination of *Bendinelli* and *Pfieffer* would not be made when *Bendinelli* is considered as a whole. "It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art." *In re Hedges*, 228 U.S.P.Q. 685, 687 (Fed. Cir. 1986). When *Bendinelli* is examined as a whole, *Bendinelli* teaches one of ordinary skill in the art that program code provided to a user may be provided to a user as, for example, Extensible Markup Language (XML), in the form of a disk. Therefore, when *Bendinelli* is considered as a whole, the sole purpose taught or suggested for XML is a program code and information needed to establish a VPN.

When *Pfieffer* is examined as a whole, *Pfieffer* teaches one of ordinary skill in the art that a DTD file is a grammer that describes what tags and attributes are valid in an XML document. The purpose of the DTD file, as disclosed by *Pfeiffer*, is to define, or constrain new tags in XML by writing a DTD file. Therefore, when *Pfeiffer* is considered as a whole, *Pfeiffer* merely teaches use of a DTD file to check validity of an XML. Thus, *Bendinelli* and *Pfieffer*, when considered as a whole, fail to teach or suggest establishing a security policy specification format as a DTD file for the purpose of

defining a configuration of an IP security tunnel, as in claim 2. Therefore, the proposed combination of the references would not be made when the references are considered as a whole.

Even if the references could be properly combined, the combination of the references would not form the presently claimed invention. The present invention is directed towards establishing a security policy specification format as a DTD file for automatically configuring IP security tunnels. A combination of *Bendinelli* and *Pfieffer* would not form the presently claimed invention in claim 2. Instead, a combination of the references would merely result in an XML document containing program code and information for establishing a VPN and a DTD file that determines the validity of the XML file. Thus, any alleged combination of *Bendinelli* and Pfeiffer would not be sufficient to form the claimed invention as recited in claims 2-4, 15-17, and 28-30.

Furthermore, a proper prima facie case of obviousness must be supported by some teaching, suggestion or motivation contained in the prior art. The Examiner not provided a proper motivation to combine the different elements from *Bendinelli* and *Pfieffer*. The Examiner states that it would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Pfeiffer with those of Bendinelli and add the use of DTD files with XML files to increase organization and allow for validation of an XML file. However, the motivation for the combination of *Bendinelli* and *Pfeiffer* is not based on any rationale, suggestion or motivation provided by the references. The Examiner is merely stating that it would be better to combine the references, without offering any support or suggestion for the combination of the references.

Furthermore, there is absolutely no motivation found in either reference to use a DTD file for a security policy specification format. The Examiner may not merely state that the modification would have been obvious to one of ordinary skill in the art without pointing out in the prior art a suggestion of the desirability of the proposed modification. There is no suggestion in either *Bendinelli* or *Pfieffer* to establish a security policy specification format as a DTD file, as is claimed in claim 2. Furthermore, although *Bendinelli* mentions use of XML for program code, *Bendinelli* does not teach, suggest or motivate establishing a security policy specification format as a DTD file or generating

an XML file utilizing a plurality of elements within a DTD file, as in the presently claimed invention, as in claims 2-4, 15-17, 28-30. Therefore, the Examiner has failed to set forth a suggestion or motivation for the alleged combination of *Bendinelli* and *Pfieffer*.

Moreover, the Examiner may not use the claimed invention as an "instruction manual" or "template" to piece together the teachings of the prior art so that the invention is rendered obvious. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Such reliance is an impermissible use of hindsight with the benefit of applicant's disclosure. *Id.* Therefore, absent some teaching, suggestion, or incentive in the prior art, *Bendinelli* and *Pfieffer* cannot be properly combined to form the claimed invention. As a result, absent any teaching, suggestion, or incentive from the prior art to make the proposed combination, the presently claimed invention can be reached only through the impermissible use of hindsight with the benefit of applicant's disclosure a model for the needed changes.

Moreover, even assuming *arguendo* that the modification proposed by the Examiner were obvious, *Bendinelli* and *Pfieffer* do not teach or fairly suggest the combination of features recited in dependent claim 2. Dependent claims 15 and 28 recite subject matter addressed above with regard to claim 2 and are allowable under the same rationale. At least by virtue of their dependency on claims 2, 15, and 28, dependent claims 3-4, 16-17, and 29-30 are patentable over any alleged combination of *Bendinelli* and Pfeiffer for the same reasons set forth above with respect to claims 2, 15, and 28. Therefore, the rejection of claims 2-4, 15-17 and 28-30 under 35 U.S.C. § 103(a) has been overcome.

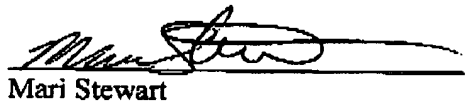
VI. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: July 20, 2005

Respectfully submitted,



Mari Stewart
Reg. No. 50,359
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants